EXAMINER'S AMENDMENT

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims

Claim 1 (Currently amended): A method for accommodating a legacy application, the legacy application resident on a legacy system having provisions for a low-level credential authorization model which employs username-and-password based authorization, the method comprising:

obtaining a request from a high-level credential authorization model for a high-level credential to be provided by the legacy application, wherein the high-level credential authorization model does not employ username-and-password based authorization;

retrieving the requested high level credential from a database of credentials; and

marshaling the requested high-level credential, the marshaling is characterized by converting a description of the high-level credential into a format recognizable as a low-level credential by the legacy application employing a low-level credential authorization model, wherein the marshaling is a mechanism by [[a]]which a description of the high-level credential is passed through a secured operating system layer using an interface designed to output low-level credentials.

Claim 2 (Canceled)

Claim 3 (Original): A method as recited in claim 1, wherein a high-level credential is a credential selected from a group composed of X.509 Certificates and bio-metrics.

Claim 4 (Currently amended): A method as recited in claim 1, wherein the marshaled credentials appear to be a conventional username[[/]] and password pair to the legacy application.

Claim 5 (Currently amended): A method as recited in claim 1, wherein marshaling comprises:

obtaining the requested high-level credential;

converting the requested high-level credential to generate a low-level credential that represents the requested high-level credential while appearing to be a conventional username[[/]]and password pair to the legacy application.

Claim 6 (Original): A method as recited in claim 1, wherein the legacy application never has access to the high-level credential.

Claim 7 (Original): A computer-readable medium having computer-executable instructions that, when executed by a computer, perform a method as recited in claim 1.

Claim 8 (Currently amended): In a computing environment where ~~certain~~ legacy processes have a provision for low-level credentials but have no provision for high-level credentials, wherein a provision for low-level credentials employs username-and-password based authorization while a provision for high-level credentials does not employ username-and-password based authorization, a method for accommodating such processes comprising:

obtaining a request for a credential from a legacy process, wherein the requested credential is a high-level credential, which is not username-and-password based;

retrieving the requested credential from a database;

converting the requested high-level credential into a format approximating a low-level credential and representative of the requested high-level credential; and

passing a description of the high-level credential through a secured operating system layer using an interface designed to output low-level credentials.

Claim 9 (Original): A method as recited in claim 8, wherein a high-level credential is a credential selected from a group composed of X.509 Certificates and bio-metrics.

Claim 10 (Currently amended): A method as recited in claim 8, wherein the converted credentials appear to be a conventional username[[/]]and password pair to the legacy process.

Claim 11 (Currently amended): A method as recited in claim 8, wherein the legacy process never has access to the high-level credential.

Claim 12 (Original): A computer-readable medium having computer-executable instructions that, when executed by a computer, perform a method as recited in claim 8.

Claim 13 (Currently amended): A method for authenticating a user to a network, the method comprising:

using an interface designed to output low-level credentials;

obtaining a request for a high-level_credential to authenticate the user to access a resource within the network, wherein the resource requires an appropriate high-level credential before the user may access the resource;

locating the appropriate high-level_credential;

passing a description of the high-level credential, ~~in place of the low level credential,~~ through a secured operating system layer using ~~an~~ said interface so high-level credential is formatted as a ~~designed to output~~ low-level credential~~s~~,

returning the appropriate high-level credential to the resource within the network, so that the resource allows the user to access such resource;

wherein the obtaining, locating, and returning, and passing are performed without user interaction so that the user need not be aware that such steps are being performed.

Claim 14 (Original): A method as recited in claim 13 further comprising repeating the obtaining, locating, and returning for a different network that is authenticated using a different credential.

Claim 15 (Original): A computer-readable medium having computer-executable instructions that, when executed by a computer, perform a method as recited in claim 13.

Claims 16-17 (Canceled)

Claim 18 (Currently amended): A credential management architecture, comprising:

a trusted computing base (TCB) that has full access to persisted credentials, the TCB being configured to interact with an untrusted computing layer (UTCL) that accesses the persisted credentials via the TCB,

the TCB comprises:

a credential management module configured to receive requests from the UTCL for a high-level credential for a resource, the high-level credential being associated with a user and not being username-and-password based authorization;

a credential database associated with the user, wherein credentials are persisted within the database;

the credential management module being configured to retrieve credentials from the database; and

an interface that performs marshaling, wherein marshaling is characterized by converting a description of the high-level credential into a format recognizable as a low-level credential by the legacy application. ~~for~~

~~passing a description of a high-level credential, in place of the low-level credential, designed to output low-level credentials,~~

Claim 19 (Canceled)

Claim 20 (Currently amended): An architecture as recited in claim 18, wherein the marshaled credentials appear to be a conventional username[[/]]and password pair to the UTCL.

Claim 21 (Original): A computer-readable medium having computer-executable instructions that, when executed by a computer, employ an architecture as recited in claim 18.

Claim 22 (Original): An operating system embodied on a computer-readable medium having computer-executable instructions that, when executed by a computer, employ an architecture as recited in claim 18.

Claim 23 (Currently amended): An apparatus comprising:

a processor;

a marshaler executable on the processor to:

obtain a high-level credential, wherein a high-level credential is employed in an authorization model which is not username-and-password based authorization;

convert the high-level credential to generate a representation of the high-level credential that is formatted as a low-level credential so that it appears to be a conventional username[[/]]and password pair; and

pass a description of the high-level credential through a secured operating system layer using an interface designed to output low-level credentials.

Claim 24 (Currently amended): An accommodation system comprising:

a request obtainer configured to obtain a request for a high-level credential from a low-level-credential-application, wherein low-level credentials utilizes username-and-password based authorization while high-level credentials do not employ username-and-password based authorization;

a credential retriever configured to retrieve the requested credential from a database of credentials;

a marshaler configured to marshal the requested credential and return the marshaled credential to the low-level-credential-application, wherein marshaling performed by the marshaler is characterized by converting a description of the high-level credential into a format recognizable as a low-level credential by the low-level-credential-application employing a low-level credential authorization model and ~~passiong~~ passing a description of the high-level credential through a secured operating system layer using an interface designed to output low-level credentials.

Claim 25 (Original): A system as recited in claim 24, wherein a high-level credential is a credential selected from a group composed of X.509 Certificates and bio-metrics.

Claim 26 (Currently amended): A system as recited in claim 24, wherein the marshaled credentials appear to be a conventional username[[/]]and password pair to the legacy application.

Claim 27 (Canceled)

Claim 28 (Previously presented): A system as recited in claim 24, wherein the low-level-credential-application never has access to the high-level credential.

Claim 29 (Currently amended): A system for authenticating a user to a network, the system comprising:

a request obtainer configured to obtain a request for a high-level credential to authenticate the user to access a resource within the network, wherein the resource requires an appropriate credential before the user may access the resource, wherein a high-level credential do not utilize username-and-password based for high-level credential authorization;

a credential retriever configured to retrieve the appropriate high-level credential from a database of credentials;

a credential marshaler configured to generate a representation of the high-level credential formatted as a low-level credential so that it appears to be a conventional username[[/]]and password pair to a low-level-credential-application, wherein a low-level credential utilizes username-and-password based authorization, and pass a description of the high-level credential through a secured operating system layer using an interface designed to output low-level credentials; and.

a credential returner configured to return the marshaled high-level credential to the resource within the network, so that the resource allows the user to access such resource;

wherein the obtainer, retriever, marshaler, and returner are further configured to operate without user interaction.

Claim 30 (Original): An operating system comprising a system as recited in claim 29.

Claim 31 (Original): A network environment comprising a system as recited in claim 29.

Claim 32 (Previously presented): An application programming interface (API) method comprising:

receiving a CredUI-promptfor-credentials call having a set of parameters comprising a TargetName, Context, AuthFlags, and Flags;

retrieving the parameters from the call to determine a specified resource;

obtaining a high-level credential;

associating the high-level credential with the specified resource;

persisting the high-level credential into a database while maintaining the credential's association with the specified resource; and

passing a description of a high-level credential, in place of the low-level credential, through a secured operating system layer using an interface designed to output low-level credentials.

Claim 33 (Original): A method as recited in claim 32, wherein the set of parameters further comprises an indicator of a data structure containing customized information to display in conjunction with a user interface.

Claim 34 (Currently amended): An application programming interface (API) method comprising:

receiving a CredUI-promptfor-credentials call having a set of parameters comprising a TargetName, UserName, Password, and Flags;

retrieving the parameters from the call to determine a requesting application;

obtaining a ~~low-level credential from a user, wherein such credential includes a username and a password~~request from the application for a high-level credential; and

passing a description of a high-level credential, in ~~place of the~~a format representing a low-level credential, through a secured operating system layer using an interface designed to output low-level credentials.

Claim 35 (Original): A method as recited in claim 34, wherein the set of parameters further comprises an indicator of a data structure containing customized information to display in conjunction with a user interface.

Claim 36 (Original): A method as recited in claim 1, wherein the marshaling is performed by creating a reference to a certificate by taking a certificate hash and computing a text string for the certificate hash.

Claim 37 (Original): A method as recited in claim 1, wherein the marshaling is performed by creating a reference to credential stored in credential manager.